Has DSS Been Hacked?

Has the hot new Digital Satellite System fallen victim to signal pirates?

JOHN McCORMAC

THE RCA DIGITAL SATELLITE SYSTEM (DSS) WAS INTRODUCED with much fanfare in mid-1994. The all-digital, direct satellite broadcast system delivers high quality TV signals to satellite dishes only 18 inches in diameter. Modern data-compression technology allows a pair of geostationary satellites co-located above the equator at 101° West longitude to transmit about 150 or more high fidelity programs to the continental U.S. That number might even increase in the future.

Will the piracy that haunted large-dish, C-band satellite program delivery during the late 1980's and early 1990's do the same to the small-dish direct-satellite industry? Perhaps—the system's encryption technology is based on a modified version of the VideoCrypt conditional-access system, which has been in operation in Europe for more than five years and has been repeatedly compromised by hackers and signal pirates.

According to the information we have available, the Digital Satellite System is on the verge of being hacked. Pirate smart cards, which will give the DSS receivers access to programs, are expected be available by the time you read this.

Signal pirates are planning to make four tiers of pirate cards available. The first tier, which is expected to cost $150, will provide access to only the basic programs. The second tier card will add the subscription movie channels. The third tier card will provide access to the sports packages. The last card will give access to all services and will include a ceiling of $500 in pay-per-view (PPV) credit. Pirates are, in essence, forming an alternate access control system that will supplant the official DSS billing system with their own.

The pirate cards will contain features that will prevent them from being pirated, or at least make piracy more difficult. For example, each card will be "married" to an individual receiver or IRD (integrated receiver/descrambler). Pirates in Europe found piracy of their own cards to be a major problem. (More information on the European scrambling situation, and valuable background information on signal piracy is contained in the companion article, "Satellite Piracy: The European Experience," on page 37.)

The majority of the pirate smart cards for the European VideoCrypt system are based on the PIC16C84 microcontroller. Although that microcontroller has a code-protection fuse that normally prevents the contents of the program memory from being read out, pirates were able to "pop" the device and extract the program code of other pirates.

As a result of this, the program for hacking VideoCrypt spread rapidly throughout Europe. A repeat of this situation is the last thing that the DSS pirates want—they want to maintain control over the distribution of pirate cards. Therefore the new smart cards might be based on a more secure processor. Some pirate sources have commented that microcontrollers from Dallas Semiconductor and Zilog were under consideration.

Because of tough anti-piracy laws in the United States, the main pirate operations will be based outside of the country. Canada is rumored to be one site. Others sources have reported that operations will be based on islands in the Caribbean.

How the hack occurred

The most valuable tool for hackers is information. A valuable piece of information came from text printed on the smart card itself: "This card is the property of News Datacom Ltd. and must be returned upon request. Incorporates Videoguard (tm) security system. Provided for reception of authorized 101°W longitude satellite services. Protected by U.S Patent 4,748,668, and others."

www.americanradiohistory.com

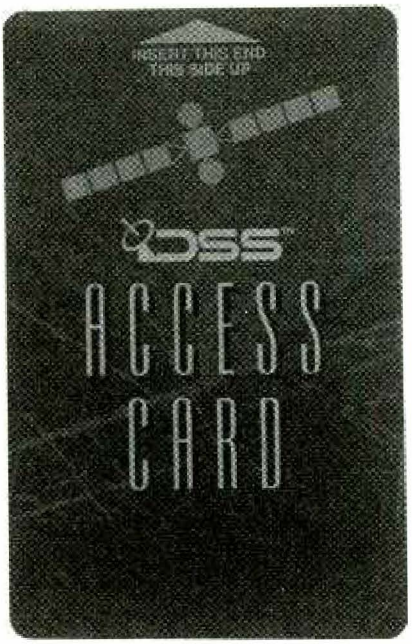
That patent referred to on the smart card is the Fiat-Shamir zero-knowledge test. It is an authentication algorithm that the decoder runs to see that the smart card inserted is a genuine smart card. The same authentication algorithm is used in the analog VideoCrypt system in Europe. This may not be the only commonality between the two systems.

In early 1984, the European VideoCrypt system, using the issue 07 card, was hacked. The full source code of the hack had been distributed freely on the Internet and via many computer bulletin board systems (BBSs). The Digital Satellite System was preparing for launch in the USA.

It was a gut-wrenching time for the executives involved in the DSS venture. The common element between Europe and the U.S. was News Datacom. The DSS executives were worried about the security of their new system. Would what happened in Europe happen in the U.S.?

Slowly but surely the favorable press coverage started. The satellite television trade press began to run articles about the new DSS system. The articles were, in hacker terms, content-free. The majority of the articles seemed to be written by clueless people without any knowledge of what really happened in Europe. One article in particular stated that VideoCrypt had been unhacked since its introduction in Europe in 1989—there was no mention of the 500,000 pirate VideoCrypt smart cards and the Omigod emulator programs that were in use. It seemed to be a replay of what had happened in Europe—the puff pieces in the trade press and the inevitable hacks.

Despite the articles, the 500,000 pirate VideoCrypt cards were very real and they forced Sky to issue a new card ten months ahead of schedule. But there was an even greater problem. The 08 card Sky had planned to launch was almost identical to the hacked 07 card. The 08 issue had to be scrapped, and the 09 card issue was released.



THE SMART CARD or access card for the DSS integrated receiver/descrambler (IRD) has drawn the attention of hackers.

There were two major differences between the 09 and the 07 Sky cards: The 09 had a different architecture and a very different algorithm. Sky started to distribute this new card in February 1994 but did not switch over to the card until May 18, 1994. That day is known as Dark Wednesday by European hackers.

The connection between those events and DSS is the timing. It would have been very convenient for News Datacom to draw heavily on the Sky 09 card for the new DSS card. Most of the ROM routines could have been easily adapted for the new system. The main changes would of course have been in the EEPROM, which contains the main cryptographic routines.

The operation to "pop" the 09 Sky card to read its contents took European hackers a few months. The hack required that the smart card be completely reverse engineered. Some preliminary code was sold in June last year at an auction in London, giving hackers a start. It took a further four months before the system was totally compromised. Perhaps the most important part of the operation was the discovery of a "back door" in the smart card's code.

When VideoCrypt was developed, the overall structure of the system was simplistic, compared with systems like VideoCipher II. It was also reliable. But the designers may never have expected the system to be required to support over two million subscribers.

As a direct result of this loading, the designer of the system, News Datacom, had to incorporate some new levels of access control into the system. Upgrading the decoders was out of the question—there were too many to track down. Most of the stand-alone decoders had long ago disappeared into mainland Europe.

News Datacom's solution proved to be both clever and stupid at the same time. The company incorporated a method of programming the card over the air. The over-the-air instructions were included in the standard access control data packets. The instructions looked just like more card identity numbers but they were not. The hackers called them "nanocommands."

The over-the-air programming scheme was clever in that it gave program suppliers more control over the cards—they could easily implement electronic countermeasures (ECMs) by updating the card's EEPROM and they could actively change the channel authorization. In effect they could even run a limited form of pay-per-view service.

Of course there is a downside to over-the-air programming: All of the security of this card relied on the hackers not finding out the core algorithm and obtaining a working knowledge of the card addressing. However, the core algorithm had been sold at auction in June 1994. The rest was only a matter of time.

The cracks in the edifice began to show, and by the end of July, VideoCrypt was crumbling. The Phoenix hack had worked. This hack relied on an understanding of how the ac-

www.americanradiohistory.com

cess control data packets were encrypted and structured. (The Phoenix hack allowed hackers to activate or reactivate all channels on Sky cards using a computer and eventually a standalone programmer.)

Naturally when Sky tried to retaliate against the Phoenix hack, it used the nanocommands. The hackers were watching. It was true electronic warfare—Sky and News Datacom versus the hackers.

Gradually the function of each nanocommand was ascertained. Even now it is difficult to believe what happened next. One nanocommand was found to read a byte from the EEPROM as the input for a round of the algorithm. Another nanocommands acted like a BREAK command that would dump the current result out as the decryption key.

The hackers had the algorithm and knew the result just prior to the byte from the EEPROM being used. They could dump out the result just after the EEPROM byte had been processed through the algorithm. Since they then had the main components, it was simply a case of starting the algorithm from the first result and stepping through with input bytes from 0 to 255. This hack has become known as the "Vampire Hack".

Of course this attack was not perfect. The resulting data from the Vampire hack of the 09 Sky card seemed to make no sense. The processor in the smart card was based on the 6805, but the data was definitely not related to the 6805. Eventually the hackers cracked the encryption and made sense out of the data.

The speed of the reported DSS hack strongly indicates that the same card type was used for the DSS system. This would mean that the same techniques that were used to pop the 09 Sky card could be used on the DSS card.

The real test of the pirate cards lies ahead. As with the European VideoCrypt, the DSS smart card may be over-the-air programmable. This would mean that the DSS cards could be updated over the air and new cards would not have to be issued immediately. The pirate cards would, of course, would need to be updated by the pirates.

The main difference between Europe and the U.S. is that the American hacking industry has experience with such upgrading. The same technology was used to hack VideoCipher II (the compromised scrambling system that was used for C-band transmissions). The pirate cards may well come with a modem module to automatically update the card.

How the Vampire Hack works

For all of its digital complexity, the European VideoCrypt system still depends on a 9600-baud data link to a smart card. The smart card is an eight-bit processor based on a 6805. It is not fast enough to run calculation-intensive algorithms such as RSA (Rivest Shamir Adelmann). As a result the VideoCrypt encryption algorithms have been register-based hashing algorithms that are designed to be fast and efficient.

In the European VideoCrypt system, two data packets are associated with the decryption process: the 74h packet and the 78h packet. The packet format and structure the DSS system uses is not yet known. However, the smart-card interface conforms to the ISO-7816 specification, so the packet types can be determined by monitoring the data.

For reasons of economy, it is possible that the packet structure that News Datacom used for DSS is similar to that for VideoCrypt. However, the actual algorithms may be slightly different.

Some of the differences between the European and DSS system are expected to be in the pay-per-view (PPV) routines. In the European VideoCrypt system, the main PPV routines were incorporated into the card-decoder interface microcontroller. This chip also held the PPV token reservoir. It is unlikely that such a mistake has been repeated in the DSS system.

In the DSS IRD, a custom microcontroller controls the interface between the card and decoder. The contents of the microcontroller's memory is protected from prying. By contrast, the designers of the European VideoCrypt system made a major mistake by not protecting the microcontroller. Hackers were able to dump out contents of the microcontroller's ROM and were able to attack the system. They rewrote the code and loaded it into a version of the microcontroller that contained EPROM. This modified code looked for the card's identity number in a switch-off packet, and ignored the packet. This

IMPORTANT
NEWS DATACOM
• Do Not Bend Access Card.
• Do Not Remove and Re-Insert Card Unnecessarily.
• Never Submerge Card In Liquid or Use Cleaning Fluids On It.
0000 0777 0928
F56227185175

THE BOTTOM OF THE SMART CARD shows its contact points. Note News Datacom's patent statement that hackers credit with helping them.

www.americanradiohistory.com

hack, known as the KENtucky Fried Chip, prevented Sky from switching off a smart card.

The card-decoder microcontroller would have been the first chip in the DSS IRD to have been reverse-engineered. The reverse engineering of a customized microcontroller is not, in most cases, as difficult as a smart card. In mass-produced IRDs and decoders, the microcontrollers are typically ROM versions of commonly available microcontrollers. Some of them have simple back doors.

Packets

The 74h message packet is the workhorse of the VideoCrypt system. It carries all of the card turn-on and turn-off codes. The packet contents are also used as the input data for the hashing algorithm that generates the decryption key.

The data in this packet has a 27-4-1 structure. The first 27 bytes contain the decoder flags, the card addressing instructions, the channel identifier and the card addresses affected by the packet. The next four bytes are a hash algorithm checksum.

When the packet is processed by the hash algorithm, part of the results in stages 28, 29, 30, and 31 should equal the checksum bytes. The card will reject packets that do not have a valid checksum. The purpose of the checksum is to prevent a third-party authorization of a smart card.

The final byte is a packet checksum. The value of this byte is that required to bring the sum of the bytes in the packet to a multiple of 256.

Byte 0 in the 74h packet carries the decoder flags. It effectively tells the decoder how to handle the packet. The high nibble (4 bits) identifies the type of scrambling in use. A value of Cxh indicates that the channel is not scrambled. A value of Exh or Fxh indicates that the channel is hard scrambled. The Dxh value may indicate a free-access mode of scrambling. The value x8h as the low nibble indicates that the packet will be used to generate a new decryption key. The value x0h indicates an information packet that should not to be used to generate a new key.

Another important element is the packet-type byte. This byte identifies the packet as being a switch-on, switch-off or ECM packet. The ECM packet carries the nanocommands. Basically speaking, the area of the packet that would normally be occupied by card-identity numbers carry a routine that is loaded into the smart card. This is the back door.

The 78h packet is the eight-byte decryption key generated by the hash algorithm in the smart card. This key is passed to the pseudo-random number generator (PRNG) in the custom integrated circuit in the European VideoCrypt decoder. Only 60 bits of this result is used to seed the PRNG.

There are four requirements for the Vampire hack. The first is a working implementation of the hash algorithm. This is necessary because the state of the answer bytes must be tracked through the whole process. The hash implementation is also required to generate a valid checksum for the packet.

The second requirement is a set of current Phoenix codes or, alternatively, the algorithm for generating these codes. These codes will be exclusive-or-ed with the packet data before the checksum is generated. Since the KENtucky Fried Chip hack, News Datacom has had to encrypt the information in the 74h packets. In order for the Vampire packets to be accepted and processed by the smart card, they have to be properly encrypted.

The third requirement is a working knowledge of the nanocommands. The basic commands in the Vampire hack are the 09h address loader, the 30h data processor and the 03h break.

It is necessary to know how many hash iterations are effected by each nanocommand. This is where much of the research work will have to be carried out with the DSS. It would be extremely lucky for the hackers if News Datacom used the same nanocommands in the DSS card.

However, if News Datacom believed that the card and the hashing algorithm could not be popped, then they may well have used similar nanocommands. The nanocommands in the 09 Sky card seem to be based on 6805 microcontroller commands.

The fourth requirement is some sort of recovery routine. This routine will exhaustively search for the data byte used in the 30h command. This is perhaps the most intensive part of the algorithm and some hackers decided to leave this recovery routine until after the results are obtained from the card.

The DSS hack will be carried out in six stages:

- Stage 1: Nanocommand generation. Basically this stage involves setting the address bytes that follow the 09h command.
- Stage 2: Encryption of packet data. This is where the Nanocommand Decrypt Key algorithm is applied to the packet data. It exclusive-ors the output of the encryption algorithm with the nanocommands and other data.
- Stage 3: Checksum generation. The packet presented to the card must have a valid checksum or the card will reject it. Again the working implementation of the hash algorithm is required. In many respects this process is similar to the original Phoenix program.
- Stage 4: Vampire packet sent to card. The circuitry used for this stage of the DSS hack is the same as that used for the Phoenix hack.
- Stage 5: Answer packet (78h) recorded. The answer packet from the card would be recorded in a file along with the address of the recorded data, the nanocommands used, and the state of the answer bytes just prior to the execution of the nanocommands.
- Stage 6: Data recovery. Theoretically this is a simple stage.

Continued on page 92

www.americanradiohistory.com

SATELLITE PIRACY

continued from page 40

that, the company began a deluge of legal action in the UK.

Sky essentially prosecuted the "small guys" who did not have the money to defend themselves. Even though the pirates were breaking the law in the UK, Sky's action was a public-relations nightmare. The company created martyrs.

In one incident, for example, Sky drew the media's attention by trying to prove that one defendant was a main dealer of Genesis blockers. However, that defendant had stocked only 300 blockers—he was certainly not one of the larger dealers.

Sky estimated that it lost 50,000 subscribers and 2.25 million pounds ($3.5 million) to piracy between January 1st and may 18th 1994. However, according to Hack Watch News, a European hacker publication, there were about 300,000 pirate Sky cards in the UK at the beginning of the year.

The 09 issue of cards in February cost Sky approximately 21 million pounds. The next card issue, 0A, that was due in April 1995, probably cost another 21 million pounds

Another card issue (OB) will probably be necessary in November 1995 if Sky wants to maintain the security of its conditional-access system. The present cycle is not short enough to deter pirates from producing their own cards.

The cloning of VideoCrypt

A sure sign that the VideoCrypt scrambling system was thoroughly defeated was that it was cloned. The clone system, called KoyCrypt, was demonstrated at the London Cable And Satellite Show in April 1994. The company that cloned it, Hi Tech Xtravision, also developed a customized smart card that it claimed would be much more difficult to hack. It seemed to be a case of a poacher turned gamekeeper.

Despite the potential benefits of KoyCrypt, broadcasters that want to use it—and perhaps have a more secure system—can't. Copyright issues prevent them from doing so.

The present day

At the time of writing, VideoCrypt is still hacked. There are a few programs available for the PC and the Macintosh that actually allow a computer to tie into a decoder and decode all of the VideoCrypt channels. These programs are free—most of the computer bulletin-board systems in Europe have copies. Today when Sky implements an ECM, the modified versions of the programs are posted on the BBSs within a few hours—an embarrassing situation for News Datacom and Sky.

Many of the pirate smart cards on the market now use pirate technology developed in the U.S. One card has a keypad. When there is an ECM, the pirate card user just telephones an answering service to retrieve a set of numbers. He then enters the numbers on the keypad and the pirate card resumes operation. Another card uses a modem.

Things could change over the next few months though if Sky brings out its new OA-issue card. Then the pirates will be defeated—at least for a little while. However, the problem is that nobody is sure how long the new card will remain unhacked. The most important lesson that the DSS programmers could learn from the European experience is that smart cards have to be changed every six months. Otherwise it's certain that they will be hacked. Ω

HAS DSS BEEN HACKED?

continued from page 36

In practice it is complex. The state of the answer bytes prior to the execution of the nanocommands is known. The process used here is an exhaustive search. The 30h and 03h iterations would be executed exhaustively with all values from 00h to FFh being tried as the input in the 30h loop. The potential for errors exists but it is the simplest way, short of reverse-engineering the card, to obtain the contents of the card memory.

On paper, these steps might look simple. In reality they are complex. The main problem hackers had with the European situation was working out how the recovered data mapped back to standard 6805 commands. Eventually, the op-codes were established and the routines began to make sense. The hackers now have a fully disassembled dump of the ROM and EEPROM of the Sky 09 smart card.

It is probable that the DSS hackers have used the Sky 09 data and knowledge to attack the DSS smart card. The problem for the DSS hackers is knowing the extent and power of the nanocommands in the DSS card. DSS may have a trick or two in its cards to send the hackers back to their drawing boards.

One thing is certain, though. If the DSS engineers do not take into account what happened in Europe, a similar series of events is sure to happen here. Ω

–LEARN ALL THE FACTS–

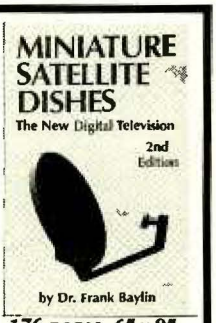
MINIATURE 18" DISHES & HACKING

320 pages, 6" x 8.5"
$50 plus $4 s/h

—TWO NEW BOOKS—
by Frank Baylin / John McCormac

- 18" satellite dish technology, players, programming, encryption and more
- The aclaimed hacker's "bible" outlines all the nitty-gritty technical details

CALL 1-800-483-2423
to order or for a catalog



176 pages, 6" x 9"
$20 plus $4 s/h

Baylin publications
1905 Mariposa, Boulder, Colorado 80302, USA
Telephone: 303-449-4551 FAX: 303-939-8720

www.americanradiohistory.com